Format du message d'audit

StorageGRID software

NetApp
December 03, 2025

Sommaire

Format du message d’audit 1
Format du message d’audit 1
Types de données 2
Données spécifiques à l’événement 2
Éléments communs aux messages d’audit 3
Exemples de messages d’audit 4

Format du message d’audit

Format du message d’audit

Les messages d’audit échangés au sein du système StorageGRID incluent des informations standard communes à tous les messages et un contenu spécifique décrivant l’événement ou l’activité signalé.

Si les informations récapitulatives fournies par le"audit-explication" et"somme d’audit" les outils sont insuffisants, reportez-vous à cette section pour comprendre le format général de tous les messages d’audit.

Voici un exemple de message d’audit tel qu’il pourrait apparaître dans le fichier journal d’audit :

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(F
C32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265006
03516]]
```

Chaque message d’audit contient une chaîne d’éléments d’attribut. La chaîne entière est entourée de crochets(`[ ]`), et chaque élément d’attribut dans la chaîne a les caractéristiques suivantes :

- Entouré de parenthèses `[ ]`
- Introduit par la chaîne `AUDT` , qui indique un message d’audit
- Sans délimiteurs (pas de virgules ni d’espaces) avant ou après
- Terminé par un caractère de saut de ligne `\n`

Chaque élément comprend un code d’attribut, un type de données et une valeur qui sont rapportés dans ce format :

```
[ATTR(type):value][ATTR(type):value]...
[ATTR(type):value]\n
```

Le nombre d’éléments d’attribut dans le message dépend du type d’événement du message. Les éléments d’attribut ne sont pas répertoriés dans un ordre particulier.

La liste suivante décrit les éléments d’attribut :

- `ATTR`est un code à quatre caractères pour l’attribut signalé. Certains attributs sont communs à tous les messages d’audit et d’autres sont spécifiques à chaque événement.
- `type`est un identifiant à quatre caractères du type de données de programmation de la valeur, tel que UI64, FC32, etc. Le type est entre parenthèses `( ) .
- `value`est le contenu de l’attribut, généralement une valeur numérique ou textuelle. Les valeurs suivent toujours deux points(:`). Les valeurs de type de données CSTR sont entourées de guillemets doubles « ».

Types de données

Différents types de données sont utilisés pour stocker des informations dans les messages d'audit.

Type	Description
UI32	Entier long non signé (32 bits) ; il peut stocker les nombres de 0 à 4 294 967 295.
UI64	Entier long double non signé (64 bits) ; il peut stocker les nombres de 0 à 18 446 744 073 709 551 615.
FC32	Constante à quatre caractères ; une valeur entière non signée de 32 bits représentée par quatre caractères ASCII tels que « ABCD ».
iPad	Utilisé pour les adresses IP.
CSTR	Un tableau de longueur variable de caractères UTF-8. Les caractères peuvent être échappés avec les conventions suivantes : • La barre oblique inverse est \\. • Le retour chariot est \r. • Les guillemets doubles sont \". • Le saut de ligne (nouvelle ligne) est \n. • Les caractères peuvent être remplacés par leurs équivalents hexadécimaux (au format \xHH, où HH est la valeur hexadécimale représentant le caractère).

Données spécifiques à l'événement

Chaque message d'audit dans le journal d'audit enregistre des données spécifiques à un événement système.

Après l'ouverture `[AUDT:` conteneur qui identifie le message lui-même, l'ensemble d'attributs suivant fournit des informations sur l'événement ou l'action décrit par le message d'audit. Ces attributs sont mis en évidence dans l'exemple suivant :

```
2018-12-05T08:24:45.921845 [AUDT:*\[RSLT\(FC32\):SUCS\]*
\[TIME\(UI64\):11454\]\[SAIP\(IPAD\):"10.224.0.100"\]\[S3AI\(CSTR\):"60025621595611246499"\]
\[SACC\(CSTR\):"compte"\]\[S3AK\(CSTR\):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dYzKlumRsK
JA=="\] \[SUSR\(CSTR\):"urn:sgws:identity::60025621595611246499:root"\]
\[SBAI\(CSTR\):"60025621595611246499"\]\[SBAC\(CSTR\):"account"\]\[S3BK\(CSTR\):"bucket"\]
\[S3KY\(CSTR\):"object"\]\[CBID\(UI64\):0xCC128B9B9E428347\] \[UUID\(CSTR\):"B975D2CE-E4DA-
4D14-8A23-1CB4B83F2CD8"\]\[CSIZ\(UI64\):30720\][AVER(UI32):10]
\[ATIM(UI64):1543998285921845]\[ATYP\(FC32\):SHEA\][ANID(UI32):12281045][AMID(FC32):S3RQ]
\[ATID(UI64):15552417629170647261]]
```

Le `ATYP` L'élément (souligné dans l'exemple) identifie quel événement a généré le message. Cet exemple de message inclut le"KARITÉ" code de message ([ATYP(FC32):SHEA]), indiquant qu'il a été généré par une demande S3 HEAD réussie.

Éléments communs aux messages d'audit

Tous les messages d'audit contiennent les éléments communs.

Code	Type	Description
AU MILIEU DE	FC32	ID du module : identifiant à quatre caractères de l'ID du module qui a généré le message. Cela indique le segment de code dans lequel le message d'audit a été généré.
ANID	UI32	ID de nœud : l'ID de nœud de grille attribué au service qui a généré le message. Chaque service se voit attribuer un identifiant unique au moment de la configuration et de l'installation du système StorageGRID . Cet identifiant ne peut pas être modifié.
ASES	UI64	Identifiant de session d'audit : dans les versions précédentes, cet élément indiquait l'heure à laquelle le système d'audit était initialisé après le démarrage du service. Cette valeur temporelle a été mesurée en microsecondes depuis l'époque du système d'exploitation (00:00:00 UTC le 1er janvier 1970). **Remarque :** cet élément est obsolète et n'apparaît plus dans les messages d'audit.
ASQN	UI64	Nombre de séquences : dans les versions précédentes, ce compteur était incrémenté pour chaque message d'audit généré sur le nœud de grille (ANID) et réinitialisé à zéro au redémarrage du service. **Remarque :** cet élément est obsolète et n'apparaît plus dans les messages d'audit.
ATID	UI64	ID de trace : un identifiant partagé par l'ensemble des messages déclenchés par un événement unique.
ATIM	UI64	Horodatage : l'heure à laquelle l'événement a été généré et a déclenché le message d'audit, mesurée en microsecondes depuis l'époque du système d'exploitation (00:00:00 UTC le 1er janvier 1970). Notez que la plupart des outils disponibles pour convertir l'horodatage en date et heure locales sont basés sur des millisecondes. L'arrondi ou la troncature de l'horodatage enregistré peut être nécessaire. L'heure lisible par l'homme qui apparaît au début du message d'audit dans le `audit.log` le fichier est l'attribut ATIM au format ISO 8601. La date et l'heure sont représentées comme *`YYYY-MMDDTHH:MM:SS.UUUUUU`* , où le `T` est une chaîne de caractères littérale indiquant le début du segment de temps de la date. *`UUUUUU`* sont des microsecondes.

Code	Type	Description
ATYP	FC32	Type d'événement : identifiant à quatre caractères de l'événement enregistré. Cela régit le contenu de la « charge utile » du message : les attributs qui sont inclus.
MOYENNE	UI32	Version : la version du message d'audit. À mesure que le logiciel StorageGRID évolue, de nouvelles versions de services peuvent intégrer de nouvelles fonctionnalités dans les rapports d'audit. Ce champ permet la compatibilité descendante dans le service AMS pour traiter les messages provenant d'anciennes versions de services.
RSLT	FC32	Résultat : le résultat d'un événement, d'un processus ou d'une transaction. Si ce n'est pas pertinent pour un message, NONE est utilisé plutôt que SUCS afin que le message ne soit pas filtré accidentellement.

Exemples de messages d'audit

Vous pouvez trouver des informations détaillées dans chaque message d'audit. Tous les messages d'audit utilisent le même format.

Ce qui suit est un exemple de message d'audit tel qu'il pourrait apparaître dans le `audit.log` déposer:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPUT
][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224144
102530435]]
```

Le message d'audit contient des informations sur l'événement enregistré, ainsi que des informations sur le message d'audit lui-même.

Pour identifier quel événement est enregistré par le message d'audit, recherchez l'attribut ATYP (mis en évidence ci-dessous) :

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224
144102530435]]
```

La valeur de l'attribut ATYP est SPUT. "CRACHER" représente une transaction S3 PUT, qui enregistre l'ingestion d'un objet dans un bucket.

Le message d'audit suivant indique également le compartiment auquel l'objet est associé :

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK\(CSTR\):"s3small1"][S3
KY(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):
0][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPU
T][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):157922414
4102530435]]
```

Pour savoir quand l'événement PUT s'est produit, notez l'horodatage UTC (Universal Coordinated Time) au début du message d'audit. Cette valeur est une version lisible par l'homme de l'attribut ATIM du message d'audit lui-même :

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM\(UI64\):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):15792241
44102530435]]
```

ATIM enregistre le temps, en microsecondes, depuis le début de l'époque UNIX. Dans l'exemple, la valeur `1405631878959669` se traduit par jeudi 17 juillet 2014 21:17:59 UTC.

Informations sur le copyright

Informations sur les marques commerciales